6

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－94458

(43)公開日　平成5年(1993)4月16日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　15/21	３４０　Ａ	7218－5L			
Ｇ０６Ｋ　17/00	Ｌ	8623－5L			
Ｇ０７Ｄ　9/00	４３６　Ｚ	8513－3E			
		7130－3E	Ｇ０７Ｆ　7/08	Ｂ	
		7117－5K	Ｈ０４Ｌ　9/02	Ａ	

審査請求　未請求　請求項の数４(全 22 頁)　最終頁に続く

(21)出願番号　特願平3－278831

(22)出願日　平成３年(1991)９月30日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　真田　有

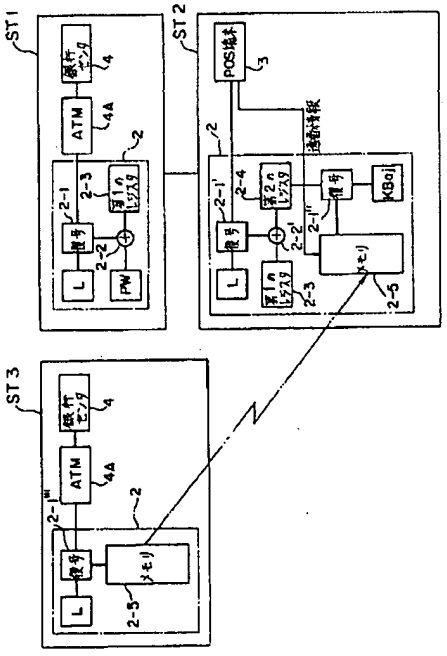
(54)【発明の名称】　電子財布システムの鍵管理方式

(57)【要約】

【目的】　本発明は、銀行センタ，現金自動支払い装置，ＩＣカード及び店舗取引端末で構成される電子財布システムを正しく運用するための認証手段に必要な鍵管理方式に関し、銀行鍵を個人毎にユニークにし、更にこれを時間可変な鍵とすることによって、高い安全性を確保できるようにすることを目的とする。

【構成】　電子財布システムの鍵管理方式において、ＩＣカード２内のメモリ２－５に、暗号化セッション鍵を複数種類記憶しておき、ＩＣカード２が店舗取引端末３側から第２の暗号化パラメータを受け取る際に、メモリ２－５のアドレス情報を有する通番情報を受け取り、この通番情報に対応するメモリ２－５のアドレスをアクセスして、対応するアドレスに記憶された暗号化セッション鍵を出力して、第２レジスタ２－４の値でこの出力を復号し、目的の認証用の鍵を得るように構成する。

本発明の原理説明図



1

【特許請求の範囲】

【請求項１】　銀行センタ（４），現金自動支払い装置（４Ａ），ＩＣカード（２）及び店舗取引端末（３）から構成され、

該銀行センタ（４）で、マスタ鍵を用いて該銀行センタ（４）が生成する第１のパラメータを暗号化し、該銀行センタ（４）より現金自動支払い装置（４Ａ）を経由してユーザの該ＩＣカード（２）へ配送すると、

ユーザは該現金自動支払い装置（４Ａ）より配送された暗号化パラメータを該ＩＣカード（２）に取り込み、該ＩＣカード（２）内のマスタ鍵で復号し、銀行発行の第１のパラメータを得、更にこのパラメータとユーザが管理するパスワードとを、該ＩＣカード（２）内で加算し、この結果を第１のレジスタ（２－３）に書き込んで、

その後、ユーザが商店で買物を行ない、該店舗取引端末（３）で買物金額を支払う際に、該ＩＣカード（２）を該店舗取引端末（３）のカードリーダへ挿入すると、該店舗取引端末（３）側で予め銀行センタマスタ鍵で暗号化した第２のパラメータを該ＩＣカード（２）に対して送り、

該ＩＣカード（２）において受信した第２の暗号化パラメータを内蔵のマスタ鍵で復号し、得られた該第２のパラメータを該第１のレジスタ（２－３）の値に対して加算し、その結果を該第２のレジスタ（２－４）に格納して、

該ＩＣカード（２）内のメモリ（２－５）に記憶された暗号化セッション鍵を用いて、該第２レジスタ（２－４）の値で復号し、目的の認証用の鍵を得るようにした電子財布システムの鍵管理方式において、

該ＩＣカード（２）内の該メモリ（２－５）に、該暗号化セッション鍵を複数種類記憶しておき、

該ＩＣカード（２）が該店舗取引端末（３）側から該第２の暗号化パラメータを受け取る際に、該メモリ（２－５）のアドレス情報を有する通番情報を受け取り、この通番情報に対応する該メモリ（２－５）のアドレスをアクセスして、対応するアドレズに記憶された該暗号化セッション鍵を出力して、該第２レジスタ（２－４）の値でこの出力を復号し、目的の認証用の鍵を得ることを特徴とする、電子財布システムの鍵管理方式。

【請求項２】　該ＩＣカード（２）の該メモリ（２－５）へ一連の暗号化セッション鍵を書き込む場合、該銀行センタ（４）よりマスタ鍵で該暗号化セッション鍵を暗号化し、このデータを該現金自動支払い装置（４Ａ）を通じて、該ＩＣカード（２）に与え、

該ＩＣカード（２）は受信したデータをマスタ鍵で復号し、得られた一連の暗号化セッション鍵データを順次該メモリ（２）に格納することを特徴とする、請求項１記載の電子財布システムの鍵管理方式。

【請求項３】　該銀行センタ（４）が暗号化セッション鍵を発行する場合、一定の時間単位に対応する複数個の暗号化セッション鍵を該現金自動支払い装置（４Ａ）経由で該ＩＣカード（２）に配送することを特徴とする、請求項１記載の電子財布システムの鍵管理方式。

2

【請求項４】　該銀行センタ（２）が該店舗取引端末（３）に対して第２の暗号化パラメータを送る場合、該銀行センタ（２）よりマスタ鍵で暗号化した第２のパラメータを一定の時間単位に対応させて複数個のデータを該店舗取引端末（３）へ送ることを特徴とする、請求項１記載の電子財布システムの鍵管理方式。

【発明の詳細な説明】

【０００１】（目次）

産業上の利用分野

従来の技術（図７，図８）

発明が解決しようとする課題（図９～図１４）

課題を解決するための手段（図１）

作用（図１）

実施例（図２～図６）

発明の効果

【０００２】

【産業上の利用分野】本発明は、銀行センタ，銀行ＡＴＭ（現金自動支払い装置），ＩＣカード及び商店ＰＯＳ端末（店舗取引端末）の要素から構成される電子財布システムにおいて、これらの構成要素を正しく運用するための認証手段に必要な鍵管理方式に関する。

【０００３】近年、テレホンカードに代表されるように、現金を直接支払わず、予め現金を各種のプリペイドカードに替えて、電話の通話料金を支払ったり、電車の切符を購入したり、食券を購入したりするプリペイドカードシステムが普及しつつある。しかし、このような現状のカードシステムでは、特定のサービスや品物のみに利用可能であるため、一般の商品購入には不向きである。

【０００４】そこで、万能プリペイドカードとして期待されるのが、電子財布システムである。これは銀行，各種金融機関が顧客に予めＩＣカードを発行しておき、顧客が買物をする際、ＡＴＭ（現金自動支払機）より、現金の代わりに金額データをＩＣカードに書き込み、顧客は店で買物した金額をこのＩＣカードにより支払うシステムである。

【０００５】かかる電子財布システムは顧客が現金を所有する必要がない点、及び店から銀行に売上げ金を運搬する現金輸送車が不要である点等から安全性が高く、効率的である。しかし、これはあくまでもＡＴＭ，ＩＣカード及び店のＰＯＳ（Ｐｏｉｎｔｏｆ　Ｓａｌｅ）システムが全て安全であることが前提である。

【０００６】

【従来の技術】図７はＩＣカードを用いたプリペイドカード・システムの従来方式のシステム構成図である。このシステムは、ＩＣカード８１，ＩＣカード８１を持っ

ているユーザが買物をする店舗に置く店舗取引端末（ＰＯＳ端末）８２，銀行センタ８３からなる。

【０００７】銀行センタ８３には、ＩＣカード８１を保有するユーザの個人口座８４、カード・ユーザが自身のカードに入金した金額データを格納しておく個人カード残高ログファイル８５、複数のカードにユーザが入金した金額の合計額を格納しておく未決済資金ファイル８６、各店舗の一定期間のカード売上合計額を未決済資金ファイルから資金移動する店舗口座８７がある。未決済資金ファイル８６は銀行センタ８３で一つまたは数個存在する。また、個人口座８４および個人カード残高ファイル８５はＩＣカード８１を保有する各個人に対応して存在し、また、店舗口座８７は各店舗に対応して存在する。

【０００８】ＩＣカード８１には、残高格納レジスタ８８があり、該ＩＣカード８１で使用可能な金額が格納されている。また、店舗取引端末（ＰＯＳ端末）８２には、該端末での売上を格納する売上データ８９が存在する。

【０００９】カード・ユーザは、自身のＩＣカード８１を使用するにあたって、まず、ＩＣカード８１に入金する。入金の際には、カードのキーパッドから暗証番号を入力し、該ＩＣカード８１を活性化させたうえ、ＡＴＭ９０を介して銀行センタ８３にアクセスする。カードに入金したい金額が個人口座８４の残高以内ならば、この金額をカード残高と加算して加算結果をＩＣカード８１の残高格納レジスタ８８にＡＴＭ９０を介して書き込む（カードへの入金金額９１）。これと同時に、カード残高を銀行センタ８３の個人カード残高ログファイル８５に書き込む。

【００１０】この個人カード残高ログファイル８５はＩＣカード８１への不正行為防止に使用できる。すなわち、カード・ユーザが次に入金にきたときにはＩＣカード８１の残高は該個人カード残高ログファイル８５に書き込まれている金額と同じかあるいは少ないはずなので、もしＩＣカード８１の残高格納レジスタ８８の金額の方が個人カード残高ログファイル８５よりも多いならばＩＣカード８１を不正改ざんしたとみなすことができる。また、個人カード残高ログファイル８５に格納されている金額は、カードを破損した場合などにガード・ユーザに対して保証する保証金額となる。

【００１１】ＩＣカード８１で買物をする場合には、店舗取引端末８２に買物金額を入力し、さらにＩＣカード８１を店舗取引端末８２に挿入し、ＩＣカード８１のキーパッドから暗証番号を入力することによりＩＣカード８１を活性化する（買物のための活性化９２）。これによって、店舗取引端末８２がＩＣカード８１の残高格納レジスタ８８の残高から買物金額を差し引いて残高額を更新する（残高減算９３）とともに、売上データ８９に買物金額を加算する。すなわち、ＩＣカード８１のカード・ユーザがＡ銀行に口座を有している場合には、売上データ８９のうちＡ銀行について、金額ａに買物金額を加算して更新する。

【００１２】店舗取引端末８２では、以上の方法によって売上げ金額を売上データ８９に加算していき、一定期間ごとに売上データ８９の金額を暗号化して銀行センタ８３に送る。すなわち、一定期間が経った時点で、銀行ごとの売上金額（例えばＡ銀行ならば金額ａ）を暗号化し、売上（請求）データ９４として該銀行センタ（例えばＡ銀行の銀行センタ）に送る。銀行センタ８３は送られてきた売上（請求）データ９４を復号し、その金額を未決済資金ファイル８６から店舗口座８７に移す。

【００１３】図８は店舗取引端末における従来の売上合算データの更新とＩＣカード残高の更新の説明図である。買物を行なう場合には、店舗取引端末８２にＩＣカード８１を挿入し、暗証番号によりＩＣカード８１を活性化したうえ、買物金額９５を店舗取引端末８２から入力する。この買物金額９５は、店舗取引端末８２の加算器９６およびＩＣカード８１の減算器９７の入力となるとともに、ＩＣカード８１の金額表示ディスプレイ９８に出力される。これによって、ＩＣカード８１のユーザは買物金額９５の入力に誤りがないか否かを判断することができる。店舗取引端末８２の加算器９６のもう一つの入力は売上合算データ９９である。買物金額９５が入力されると、加算器９６によってそれまでの売上合算データ９９に該買物金額９５を加算し、売上合算データ９９を更新する。一方、ＩＣカード８１の減算器９７のもう一つの入力は残高格納レジスタ８８の値である。買物金額９５が入力されると、減算器９７によって残高格納レジスタ８８の値から買物金額９５を減算し、再び残高格納レジスタ８８に格納し、残高を更新する。

【００１４】以上のように、従来のプリペイドカード・システムでは、ＩＣカードの暗証番号入力により本人以外の使用を不可能にするためのアクセス制御と、店舗－銀行センタ間の回線における盗聴を防止するための暗号化が安全対策として行なわれている。

【００１５】

【発明が解決しようとする課題】しかしながら、上記の従来の方式では、店舗端末での不正に対する防御はなされておらず、プリペイドカード・システム全体としての安全性に問題がある。そこで、次のようなシステムが考えられる。

【００１６】図９はそのシステム構成図である。ＩＣカード２および店舗取引端末３についての構成を説明する。ＩＣカード２は、残高格納レジスタ８および減算器２０、金額表示部２１からなる。また、店舗取引端末３は、売上データ２２、加算器２３、暗号化部２４、暗号化部２５、比較器２６、銀行鍵２７からなる。そして、売上データ２２は、売上合算データ２８および認証子２９で構成する。

5

【００１７】カード・ユーザが買物を行ないＩＣカードで支払いをする際に、店舗取引端末３の売上データ２２の更新およびＩＣカード２の残高格納レジスタ８の更新を行ない、これに加えて不正防止処理を行なう。

【００１８】まず、ＩＣカード２による支払いに先立ち、店舗取引端末３は暗号化部２４によって、売上データ２２のなかの売上合算データ２８を銀行鍵２７で暗号化し、その結果を比較器２６に出力する。銀行鍵２７は、該店舗がＩＣカードによる販売で提携している複数の銀行について銀行ごとに用意してある暗号化用の鍵である。比較器２６では、この暗号化済みのデータと認証子２９を比較し、認証子２９作成時の売上合算データ２８が改ざんされているか否かを判定する。すなわち、比較器２６で暗号化済みデータと認証子２９が一致していればデータの改ざんはなされていないと判断し、ＩＣカード２による支払い処理を実行する。一方、一致していない場合にデータを改ざんしたものと判断し、ＩＣカード２による支払い処理は行なわずに、不正行為あるいはエラーが生じたとしてオペレータに通知する。

【００１９】改ざんされていないと判定された場合には、次の処理を実行する。まず、店舗取引端末３のキーボード等から買物金額９を入力する。そして、この買物金額９と売上データ２２中の売上合算データ２８とを加算し、加算結果を売上合算データ２８に格納して、これまでの売上合算データを更新する。また、加算結果は、暗号化部２５へも入力される。暗号化部２５で、この新売上合算データを銀行鍵２７で暗号化し、その結果を認証子２９に格納して、認証子２９の更新を行なう。

【００２０】認証子２９を作成するための暗号化処理（認証子生成）は一般の暗号化と同様の処理（例えばＦＥＡＬアルゴリズムなど）で実行する。被暗号文のうちの何ビットかを暗号化し認証文とする。例えば、１２８ビットの被暗号文のうちの６４ビットを暗号化し認証文とする。このため、認証文から被暗号文を逆生成することはできない。

【００２１】一方、ＩＣカード２にも買物金額９が入力される。買物金額９は、金額表示部２１に表示されたうえ、減算器２０の入力となる。減算器２０のもう一つの入力は残高格納レジスタ８の残高データである。減算器２０は、該残高データから今回の買物金額９を減算し、その結果を残高格納レジスタ８に格納して、残高データを更新する。

【００２２】以上に説明した第１の例では、店舗取引端末３において売上合算を求めるときに売上合算データの暗号化を行ない、売上合算データとともに認証子として格納したうえ、次回、売上合算を行なう際に前回計算し格納した売上合算データを再び暗号化し、前回格納した認証子と比較することにより、店舗取引端末３において売上合算データの改ざんをしていないか否かを判定する。これによって、店舗取引端末３における売上合算データの改ざんを防ぐことが可能である。

6

【００２３】また、この第１の例において、認証子２９を使用する代わりに暗号文を用いる方法がある。システム構成は、認証子２９の部分が暗号文に代わるほかは、図９の第１の例と同様である。

【００２４】店舗取引端末３の売上合算データ２８を買物客の購買にともなって更新するに際しては（買物による加算）、まず、更新前の売上合算データ２８を暗号化部２４によって銀行鍵２７を使って、暗号化し、暗号化した文と該売上合算データに対応する暗号文が一致するか否かを判定する。一致すれば売上合算データ２８の改ざんはないと判定して更新処理を実行し、一致しない場合には改ざんあるいはエラーが生じたとして更新処理を行なわず、その旨をオペレータに通知する。ここでは、売上合算データ２８を暗号化して対応する暗号文との一致不一致を判定したが、暗号文を使用する場合には、暗号文から元の文を逆生成（復号）することが可能なので、暗号文を銀行鍵２７を使用して復号し、復号値と売上合算データ２８の一致不一致を判定してもよい。この場合も一致の場合は改ざん無し、不一致の場合は改ざん有りとみなすことができる。暗号化には、例えば、ＦＥＡＬアルゴリズム等を使用することが可能である。

【００２５】一致して、改ざんがないと判定された場合の更新処理では、まず、店舗取引端末３のキーボード等から入力された買物金額９と売上合算データ２８のデータを加算器２３で加算し、再び売上合算データ２８に格納する。また、加算器２３の出力、すなわち、新たな売上合算データを暗号化部２５に入力し、銀行鍵２７で暗号化して暗号文を作成し、これを売上合算データ２８に対応した暗号文として格納する（認証子２９の部分を暗号文として置き換える）。

【００２６】ＩＣカード２側の処理は前記の第１の例と同一である。すなわち、店舗取引端末３に入力される買物金額９がＩＣカード２にも送られ、この金額が金額表示部２１に出力されるとともに、減算器２０に入力され、減算器２０では残高格納レジスタ８の値から該買物金額９を減算して、減算結果を再び残高格納レジスタ８に格納し、残高データを更新する。

【００２７】図１０は第２の例のシステム構成図である。売上合算データの更新処理および暗号化をＩＣカード側で行なうものである。ＩＣカード２には、ＩＣカードによる合算データ暗号化部３０およびＩＣカードによるカード残高更新部３１がある。ＩＣカードによる合算データ暗号化部３０は、カード・ユーザが買物をする店舗の店舗取引端末３の売上合計金額を更新するとともに、そのデータを暗号化する処理を実行し、ＩＣカードによるカード残高更新部３１は、該ＩＣカード２の残高を更新する処理を実行する。

【００２８】ＩＣカードによる合算データ暗号化部３０は、金額表示ディスプレイ２１のほか、加算器３２、暗

号化部３３、復号部３４、比較器３５、銀行鍵格納部３６からなる。銀行鍵格納部３６には、ＩＣカード２を発行した銀行（銀行Ａ）の銀行鍵が格納してあり、この鍵を使用して、暗号化部３３では被暗号文の暗号化を行ない、復号部３４では暗号文の復号を行なう。一方、ＩＣカードによるカード残高更新部３１は、上記第１の例におけるＩＣカード２の構成と同様であり、残高格納レジスタ８および減算器２０よりなる。

【００２９】一方、店舗取引端末３は売上データ格納部３７および加算器３８、比較器３９で構成する。売上データ格納部３７は、取引銀行名４０および売上合算データの平文４１、売上合算データの暗号文４２からなり、店舗取引端末３が取引している銀行ごとに分けて格納する（３７－１，３７－２，３７－３，・・・）。そして、売上合算データ（平文４１）とそれを暗号化した暗号文４２を対にして売上データ格納部３７に格納する。

【００３０】買物客の購買によって売上合算を更新する場合には、まず、店舗取引端末３にＩＣカード２を挿入し、店舗取引端末３のキーボード等から買物金額９を入力する。ＩＣカード２を挿入したことで、ＩＣカード２にＩＣカード２を発行した銀行（ここでは銀行Ａ）について売上データ格納部３７の平文４１（４１－１）と暗号文４２（４２－１）が送られる。そして、暗号文４２はＩＣカード２内の復号部３４の入力となり、ＩＣカード２が銀行鍵格納部３６に格納している銀行鍵（ここではＡ銀行の鍵）を使用して、復号する。これによって、暗号文４２は暗号化前の平文に戻るはずである。復号化済みの文は比較器３５の入力となる。比較器３５のもう一つの入力は、店舗取引端末３から送られた平文４１である。比較器３５は復号化済みの文と店舗取引端末３からの平文４１を比較し、一致していれば店舗取引端末３側での売上データの改ざんはないとみなし、売上合算データの更新処理を行なう。一方、一致していない場合には、復号化した文ともとの平文が異なるということで、何らかの改ざんあるいはエラーが発生したものとしてオペレータにその旨を通知し、処理を終了する。

【００３１】比較器３５の結果が一致で、改ざんされていない場合には、店舗取引端末３から送られてきた売上データ格納部３７内の平文４１の値と、キーボードで入力した買物金額９を加算器３２に入力する。加算器３２はこれらの二つの値を加算して売上合算金額を求める。この結果は、店舗取引端末３に送られるとともに、ＩＣカード２内にある暗号化部３３に送られる。暗号化部３３は、銀行鍵格納部３６に格納されている銀行鍵によって売上合算金額を暗号化し、その結果を暗号文更新データ４３として店舗取引端末３に送る。店舗取引端末３では、受け取った暗号文更新データ４３を売上データ格納部３７の暗号文４２に格納する。

【００３２】一方、ＩＣカード２内の加算器３２の出力（売上合算金額）は店舗取引端末３にも送られ、店舗取

引端末３内の比較器３９の一方の入力となる。また、店舗取引端末３内にも加算器３８が存在し、売上データ格納部３７の売上データの平文４１と買物金額９を加算し、独自に売上合算金額を算出し、これを比較器３９のもう一方の入力とする。ＩＣカード２から送られてきた売上合算金額と、店舗取引端末３で独自に計算した売上合算金額とが一致すれば、正しく計算されているものとして、該売上合算金額を金額更新データ４４として売上データ格納部３７の平文４１に格納する。一方、比較器３９で不一致になれば、ＩＣカード２から送られてきた売上合算金額と、店舗取引端末３で独自に計算した売上合算金額とが異なることになり、ＩＣカード２側あるいは店舗取引端末３側のいずれか、あるいは両方でエラーが発生していることになる。このような場合には処理を停止し、その旨を出力する。

【００３３】ＩＣカード２では、店舗側の売上合算データ更新処理に加えて、自身の残高更新処理も行なう。ＩＣカードによるカード残高更新部３１は、残高格納レジスタ８に格納してある残高データを減算器２０に入力する。そして、減算器２０のもう一方の入力を買物金額９とし、残高データから買物金額９を減算して、再び残高格納レジスタ８に格納する。これにより、残高データの更新が完了する。

【００３４】この第２の例は、店舗側の売上合算計算処理および売上合算の暗号化をＩＣカード側で行ない、店舗側では処理できないようにしている。前記の第１の例では、銀行鍵を店舗側で解読すれば売上合算計算およびその暗号化が可能で、不正改ざんの可能性が残されていたが、この第２の例のように、ＩＣカード側で処理させることにより、このような不正行為は防止できるようになる。また、銀行ごとに銀行鍵を変えることにより、その銀行が発行したＩＣカードでないと暗号化処理が行なえず、安全性が増すとともに、銀行鍵の更新を銀行ごとに行なえるという利点がある。

【００３５】なお、この第２の例は、暗号化処理により、売上合算データの平文４１とともに対応する暗号文４２を売上データ格納部３７に格納したが、売上合算データの平文４１の一部を使用して暗号化することにより、対応する認証子を暗号文４２のところに格納する方法を採ってもよい。

【００３６】ところで、図１１は前述の第１あるいは第２の例のシステム構成で求め、店舗取引端末に格納された売上合算データで発生し得る不正の説明図である。店舗取引端末３に蓄積されている売上データ２２は、一定期間内の売上合算データ２８と、該売上合算データ２８に暗号化処理を施して得られた認証子２９からなる。

今、ある月の売上合算データ２８が１００万円であったとする。そして、その月には、この売上合算金額を銀行センタ４に請求する（第ｎ回請求データ４８）。即ち、第ｎ回請求データ４８は売上合算データ２８（１００万

9

円）と対応する認証子２９である。銀行センタ４はこのデータを受け取り、まず、暗号化部４５が売上合算データ２８を銀行鍵４６で暗号化する。この暗号化で得た認証子を比較器４７に入力し、送られてきた認証子２９と比較する。これが一致していれば不正はないと判定し、銀行センタ４は請求額を店舗口座に入金する。

【００３７】ここで、次の月の売上合算金額が例えば１０万円と少なく、売り上げの水増しを図るために、店舗側取引端末３でこの月の売上データ２２として前月の売上データ２２をそのまま複写する不正改ざんをするものとする。すなわち、前月の売上合算データ２８（１００万円）と対応する認証子２９を今月の売上データ２２として複写する。

【００３８】このような場合、第ｎ＋１回請求データ４９として複写した前月の売上データ２２がそのまま銀行センタ４に送られる。すなわち、売上合算データ２８（１００万円）とそれに対応する認証子２９が送られる。銀行センタ４では、送られてきた第ｎ＋１回請求データ４９の売上合算データ２８を銀行鍵４６で暗号化し、認証子２９と比較する。しかし、送られてきた売上合算データ（１００万円）２８と認証子２９は対応がとれているので、前月のデータを複写したことは検出できず、このような不正を防ぐことができない。このような、複写による不正は銀行センタ４への請求時でも、月の途中でも、いつでも可能である。

【００３９】これは、売上合算データと認証子が１対１に対応していることによる。このような不正を防ぐために、売上データ２２に請求のシリアル番号を付加する方法が考えられる。

【００４０】図１２は第三の例、すなわち、売上データにシリアル番号を付加したシステムの説明図である。店舗取引端末３は銀行センタ４への売上請求ごとにインクリメントされるカウンタを有しており、銀行センタ４には各店舗取引端末に対応したシリアル番号がチェック用カウンタ５１として格納されている。そして、請求データとしては売上合算データ２８および認証子２９を送る。この認証子２９は、売上合算データ２８にシリアル番号５０を付加したデータをＩＣカード２が暗号化して得たものである。

【００４１】例えば、２回目の請求データは売上合算データ２８の値が「１００万円」であり、また、認証子２９はシリアル番号「２」と売上合算データ「１００万円」を合わせたデータを暗号化して得た認証子である。銀行側では、２回目の請求であることをチェック用カウンタ５１で検出し、これと送られてきた売上合算データ「１００万円」を合わせて暗号化し認証子を得て、店舗取引端末３から送られてきた認証子と比較する。一致していれば不正はないと判断して請求額を店舗口座に入金する。不一致ならば不正またはエラーがあると判断する。

10

【００４２】ここで、３回目の請求時に売上が少なく、店舗側取引端末３で前回の請求データを複写する不正を行なうものとする。すなわち、売上合算データ「１００万円」と認証子を複写する。銀行センタ４に請求すると、チェック用カウンタ５１により、銀行側は３回目の請求であることを検出し、シリアル番号“３“と売上合算データ「１００万円」を合わせて暗号化し認証子を求め、店舗取引端末３から送られてきた認証子と比較する。この場合、送られてきた認証子はシリアル番号「２」として暗号化したものであり、銀行センタ３で求めた認証子とは一致しない。これにより不正が検出できる。

【００４３】この第三の例では、銀行への請求回数を示すシリアル番号を売上合算データに加えて暗号化を行なったが、シリアル番号の代わりに合算開始時の日時を用いてもの実現できる。店舗取引端末３では、合算開始時の日時を売上合算データ２８に付加し、認証子を生成する。銀行センタ４では、前回の請求時に送られてきた売上合算データに付加されていた日時を店舗取引端末ごとに管理しており、今回請求された売上データに付加されている日時と比較する。日時が同じであったり、前回の請求時の日時よりも古いならば不正があると判断される。日時が新しいならば、日時と売上合算データを合わせて暗号化し、認証子を生成し、店舗取引端末から送られてきた認証子と比較し、一致していれば決済処理を行なう。一致しない場合には、何らかの不正あるいはエラーがその他にも存在すると判断され、決済処理は行なわない。

【００４４】図１３は第三の例までのシステムでも起こり得る不正の説明図である。店舗側に複数台の店舗取引端末があるとする（３－１，３－２）。店舗取引端末Ａ３－１の売上合算データ２８－１が１００万円であり、店舗取引端末Ｂ３－２の売上がったデータ２８－２が１０万円であるとする。それぞれの認証子（２９－１，２９－２）は、それぞれの売上合算データ（２８－１，２８－２）を暗号化して得たものである。

【００４５】ここで、店舗取引端末Ｂ３－２の売上が少ないので、店舗取引端末Ａ３－１の売上データ２２－１を複写して水増しする不正を行なうものとする。これによって、店舗取引端末Ｂ３－２の売上データ２２－２には、店舗取引端末Ａ３－２の売上データ2.2－１がそのまま複写され、店舗取引端末Ｂ３－２の売上も１００万円ということになる。この請求データ６１を銀行センタ４に送ると、銀行センタ４の暗号化部４５が店舗取引端末Ｂの請求データ６１中の売上合算データ２８－２（１００万円）を銀行鍵４６で暗号化し、その結果を比較器４７で送られてきた認証子２９－２と比較する。銀行センタ４は、請求データ６１からは店舗取引端末の違いを検出することができないので、比較器４７では一致すると判定され、決済処理が実行される。以上のように、他

の店舗取引端末の売上合算を複写することにより売り上げを水増しする不正が起こり得るのである。

【００４６】図１４は第４の例、すなわち、店舗取引端末のＩＤを付加するシステムの説明図である。店舗取引端末にはユニークなＩＤが与えられており、売上データ２２に店舗取引端末ＩＤ７０として含め、銀行センタ４に請求する。銀行センタ４では各端末のＩＤを管理している（端末番号７１）。

【００４７】各店舗取引端末では、売上合算データ２８に端末ＩＤ７０を付加したデータに対しての認証子２９をＩＣカードにより計算し、格納する。銀行センタ４に売上請求を行なう場合には、売上合算データ２８と認証子２９を送る。銀行センタ４では、同一の店舗取引端末ＩＤをもつ売上請求があるか否かを判定し、同じＩＤの付いた請求があれば不正があると判断する。同じＩＤの付いた請求がないならば、送られてきた売上合算データ２８を暗号化部で暗号化し、得た認証子を店舗取引端末から送られてきた認証子と比較する。一致していれば不正はないものとして決済処理を行なう。一致しない場合には、何らかの不正あるいはエラーがあるものとして決済処理を行なわないようにする。

【００４８】これによって、ＡＴＭ等の入金端末、店舗取引端末での不正が困難になり、安全性を向上することが可能である。さらに、これまで安全性の面で換金性のないプリペイドカード（目的が限られたプリペイドカード）しか発行できなかったが、換金性をもつＩＣカードが発行可能となり、キャッシュレス・システムの使用範囲が広がる。

【００４９】このようにして、カードを発行する銀行センタ及びＩＣカードを信頼点として電子財布システムを構築してきたが、万一のＩＣカードの不正な複製が可能となった場合、被害が拡大するおそれがあり、このためシステムの安全性向上化が必要とされている。

【００５０】ところで、ＩＣカードに書き込まれた秘密の鍵が、カードを発行した銀行管理の鍵（銀行鍵）と共通で、その銀行と取引する顧客のカードの鍵が全て共通であったとすると、ＩＣカードの格納された鍵が漏洩した場合、その銀行の顧客全体に被害が拡大するおそれがある。

【００５１】本発明は、このような課題に鑑み創案されたもので、銀行鍵を個人毎にユニークにし、更にこれを時間可変な鍵とすることによって、高い安全性を確保できるようにした、電子財布システムの鍵管理方式を提供することを目的とする。

【００５２】

【課題を解決するための手段】図１は本発明の原理説明図で、この図１に示す電子財布システムの鍵管理方式は、次のようなステップをとる。

（１）現金自動支払い装置４ＡとＩＣカード２との間でのステップＳＴ１。

すなわち、このステップＳＴ１では、まず、銀行センタ４で、マスタ鍵を用いて、この銀行センタ４が生成する第１のパラメータを暗号化し、この銀行センタ４より現金自動支払い装置４Ａを経由してユーザのＩＣカード２へ配送するが、次に、ユーザは現金自動支払い装置４Ａより配送された暗号化パラメータをＩＣカード２に取り込み、ＩＣカード２内のマスタ鍵Ｌを用いて復号部２－１で復号し、銀行発行の第１のパラメータを得、更にこのパラメータとユーザが管理するパスワードＰＷとを、ＩＣカード２内の加算部２－２で加算し、この結果を第１のレジスタ２－３に書き込む。

【００５３】（２）ＩＣカード２と店舗取引端末３との間でのステップＳＴ２。

すなわち、このステップＳＴ２では、ユーザが商店で買物を行ない、店舗取引端末３で買物金額を支払う際に、ＩＣカード２を店舗取引端末３のカードリーダへ挿入して、店舗取引端末３側で予め銀行センタマスタ鍵で暗号化した第２のパラメータをＩＣカード２に対して送ると、ＩＣカード２は受信した第２の暗号化パラメータを内蔵のマスタ鍵Ｌを用いて、復号部２－１′で復号し、得られた第２のパラメータを第１のレジスタ２－３の値に対して加算部２－２′で加算し、その結果を第２のレジスタ２－４に格納するが、更にＩＣカード２内のメモリ２－５に記憶された暗号化セッション鍵を用いて、第２レジスタ２－４の値を用いて復号部２－１′′で復号し、目的の認証用の鍵ＫＢａｊを得る。

【００５４】さらに詳しくは、ＩＣカード２内のメモリ２－５に、暗号化セッション鍵を複数種類記憶しておき、ＩＣカード２が店舗取引端末３側から第２の暗号化パラメータを受け取る際に、メモリ回路２－５のアドレス情報を有する通番情報を受け取り、この通番情報にに対応するメモリ２－５のアドレスをアクセスして、対応するアドレスに記憶された暗号化セッション鍵を出力して、第２レジスタ２－４の値でこの出力を復号し、目的の認証用の鍵ＫＢａｊを得る。

【００５５】（３）ＩＣカード２への暗号化鍵補給配送ステップＳＴ３。

このステップＳＴ３では、ＩＣカード２のメモリ２－５へ一連の暗号化セッション鍵を書き込む場合、銀行センタ４よりマスタ鍵で暗号化セッション鍵を暗号化し、このデータを現金自動支払い装置４Ａを通じて、ＩＣカード２に与え、ＩＣカード２は受信したデータをマスタ鍵Ｌを用いて復号部２－１′′′で復号し、得られた一連の暗号化セッション鍵データを順次メモリ２－５に格納する。

【００５６】（４）その他

銀行センタ２が暗号化セッション鍵を発行する場合、一定の時間単位に対応する複数個の暗号化セッション鍵を現金自動支払い装置４Ａ経由でＩＣカード２に配送したり、銀行センタ２が店舗取引端末３に対して第２の暗号

化パラメータを送る場合、銀行センタ２よりマスタ鍵で暗号化した第２のパラメータを一定の時間単位に対応させて複数個のデータを店舗取引端末３へ送ったりしてもよい。

【００５７】

【作用】上述の本発明の電子財布システムの鍵管理方式では、図１に示すように、まず、銀行センタ４で、マスタ鍵を用いて、この銀行センタ４が生成する第１のパラメータを暗号化し、この銀行センタ４より現金自動支払い装置４Ａを経由してユーザのＩＣカード２へ配送してから、ユーザが現金自動支払い装置４Ａより配送された暗号化パラメータをＩＣカード２に取り込み、ＩＣカード２内のマスタ鍵Ｌを用いて復号部２－１で復号し、銀行発行の第１のパラメータを得、更にこのパラメータとユーザが管理するパスワードＰＷとを、ＩＣカード２内の加算部２－２で加算し、この結果を第１のレジスタ２－３に書き込む（ステップＳＴ１参照）。

【００５８】その後、ユーザが商店で買物を行ない、店舗取引端末３で買物金額を支払う際に、ＩＣカード２を店舗取引端末３のカードリーダへ挿入して、店舗取引端末３側で予め銀行センタマスタ鍵で暗号化した第２のパラメータをＩＣカード２に対して送るが、このＩＣカード２は受信した第２の暗号化パラメータを内蔵のマスタ鍵Ｌを用いて、復号部２－１′で復号し、得られた第２のパラメータを第１のレジスタ２－３の値に対して加算部２－２′で加算し、その結果を第２のレジスタ２－４に格納して、更にＩＣカード２内のメモリ２－５に記憶された暗号化セッション鍵を用いて、第２レジスタ２－４の値を用いて復号部２－１′′で復号し、目的の認証用の鍵ＫＢａｊを得る（ステップＳＴ２参照）。

【００５９】さらに詳しくは、ＩＣカード２内のメモリ２－５に、暗号化セッション鍵を複数種類記憶しておき、ＩＣカード２が店舗取引端末３側から第２の暗号化パラメータを受け取る際に、メモリ回路２－５のアドレス情報を有する通番情報を受け取り、この通番情報にに対応するメモリ２－５のアドレスをアクセスして、対応するアドレスに記憶された暗号化セッション鍵を出力して、第２レジスタ２－４の値でこの出力を復号し、目的の認証用の鍵ＫＢａｊを得るのである（ステップＳＴ２参照）。

【００６０】ところで、ＩＣカード２のメモリ２－５へ一連の暗号化セッション鍵を書き込む場合は、銀行センタ４よりマスタ鍵で暗号化セッション鍵を暗号化し、このデータを現金自動支払い装置４Ａを通じて、ＩＣカード２に与え、ＩＣカード２は受信したデータをマスタ鍵Ｌを用いて復号部２－１′′′で復号し、得られた一連の暗号化セッション鍵データを順次メモリ２－５に格納する（ステップＳＴ３参照）。

【００６１】なお、銀行センタ２が暗号化セッション鍵を発行する場合、一定の時間単位に対応する複数個の暗

号化セッション鍵を現金自動支払い装置４Ａ経由でＩＣカード２に配送したり、銀行センタ２が店舗取引端末３に対して第２の暗号化パラメータを送る場合、銀行センタ２よりマスタ鍵で暗号化した第２のパラメータを一定の時間単位に対応させて複数個のデータを店舗取引端末３へ送ったりしてもよい。

【００６２】

【実施例】以下、図面を参照して本発明の実施例を説明する。図６は本発明の一実施例を示す全体ブロック図で、この図６に示す電子財布システムは、銀行センタ４，現金自動支払い装置（ＡＴＭ）４Ａ，ＩＣカード２及び店舗取引端末（ＰＯＳ端末）３から構成されている。

【００６３】ところで、本電子財布システムの鍵管理方式は、現金自動支払い装置４ＡとＩＣカード２と間での鍵生成パラメータ配送処理，ＩＣカード２と店舗取引端末３と間での鍵生成パラメータ配送処理，ＩＣカード２への暗号化鍵補給配送処理等に分けて説明できるが、以下各処理について詳述する。

【００６４】図２は顧客がＡＴＭ４Ａを経由して可変銀行鍵ＫＢを復号する為の鍵ＫＩＤｉを生成するのに必要なパラメータＫｃｅｎｔを配送してもらう処理を示している。この図２において、最初に顧客ＩＤｉは本人所有のＩＣカード（電子財布）２をＡＴＭ４Ａにさしこむ（図２の①）。このとき、ＩＣカード２より顧客のＩＤ番号が自動的に銀行センタ４へ送られ、銀行センタ４は送られてきたＩＤ番号を鍵テーブルのアドレスとして顧客の通信鍵Ｌｉを索引する。銀行センタ４はこの鍵Ｌｉを使って秘密パラメータＫｃｅｎｔを暗号化し、顧客ＩＤｉのＩＣカード２へ配送する（図２の②）。この手段により、銀行センタ４、ＡＴＭ４Ａ間の通路上の不在改ざんを防止することができる。

【００６５】一方、ＩＣカード２側では、カード内蔵の鍵Ｌｉで暗号化パラメータを復号部２－１で復号し、Ｋｃｅｎｔを得る（図２の③）。次に、顧客のパスワードＰＷｉとの先のＫｃｅｎｔとを加算部２－２で加算し、第２のパラメータＳｉ（＝Ｋｃｅｎｔ＋ＰＷｉ）を作り、レジスタ２－３に格納する（図２の④）。

【００６６】図３は、顧客が店で買物を行ない、買物代金をＩＣカード２で支払うときの、ＩＣカード２と店のＰＯＳ端末３と間の処理を示している。この図３において、顧客がＩＣカード２をＰＯＳ端末３のカードリーダに挿入すると、ＩＣカード２よりＩＤ番号がＰＯＳ端末３へ自動的に送出され、ＰＯＳ側のセキュリティブラックボックス（ＢＢ）３－１１より鍵ＬｉでＫｂｂを暗号化したデータＥＬｉ（Ｋｂｂ）が配送されてくる（図３の①）。ここで、ＥＬｉ（Ｋｂｂ）は銀行センタ４よりＰＯＳ端末３へ事前に配送しておく。

【００６７】一方、ＩＣカード２側ではカード内蔵の鍵Ｌｉで暗号化パラメータを復号部２－１′で復号し、Ｋ

15

ｂｂを得る（図3の②）。このＫｂｂとレジスタ2－3の格納データＳｉとを加算部2－2′で加算し、ＫＩＤｉ（＝Ｋｂｂ＋Ｋｃｅｎｔ＋ＰＷｉ）を得る（図3の③）。

【0068】次に、ＰＯＳ側セキュリティブラックボックス（ＢＢ）3－ｉｉ′よりシリアル番号（通番）ｊがＩＣカード2に対して送られ（図3の④）、ＩＣカード2側では鍵ＫＩＤｉで暗号化したｊ番目の銀行鍵ＫＢａｊをメモリ（レジスタ）2－5から索引して（図3の⑤）、更にこのデータをＫＩＤｉで復号部2－1′′で復号して、銀行鍵ＫＢａｊを得る（図3の⑥）。

【0069】そして、このようにして鍵ＫＢａｊが得られると、前記の図9～図14で説明したシステムを用いて、前述したその後の所望の処理を行なう。なお、カード内蔵の鍵ＬｉはＲＯＭに格納され、Ｓｉ格納用のレジスタ2－3，メモリ2－5としてはバッテリバックアップレジスタが使用され、ＫＩＤｉ格納用のレジスタ2－4，ＫＢａｊ用のレジスタ2－6としてはノンバックアップレジスタが使用される。そして、レジスタ2－4，2－6の内容は買物終了段階でＰＯＳ側の指示により消去される。

【0070】図4は銀行センタ4からＩＣカード2への鍵の補給処理を示している。顧客が金額データを補給する際に銀行センタ4より鍵の補給を受ける。この図4において、図2と同様に、ＡＴＭ4Ａに挿入されたＩＣカード2は銀行センタ4より、鍵Ｌｉで暗号化した暗号化銀行鍵ＥＬｉ（ＥＫＩＤｉ（ＫＢａｌ））～ＥＬｉ（ＥＫＩＤｉ（ＫＢａｎ））を配送してもらう（図4の①）。ＩＣカード2側では、鍵Ｌｉを用いて復号部2－1′′′でこれらのデータを復号して、そのデータをメモリ2－5に格納する（図4の②）。

【0071】そして、銀行センタ2が上記のように暗号化セッション鍵を発行する場合は、一定の時間単位（時間単位，日単位，週単位，月単位，年単位）に対応する複数個の暗号化セッション鍵を現金自動支払い装置4Ａ経由でＩＣカード2に配送する。今、顧客に発行する銀行鍵の変更周期例を示すと、図5のようになる。この例では、配送さる鍵は発行日から常に1年分だけもらうようになっている。

【0072】なお、銀行センタ2が店舗取引端末3に対して第2の暗号化パラメータを送る場合、銀行センタ2よりマスタ鍵で暗号化した第2のパラメータを一定の時間単位（時間単位，日単位，週単位，月単位，年単位）に対応させて複数個のデータを店舗取引端末3へ送ってもよい。

【0073】このように、ＩＣカード内蔵の銀行鍵（マスタ鍵）を個人ＩＤ又はカード発行時の時刻をＩＤとするもの等に対応する鍵を生成するメカニズムを電子財布システムに導入することにより、銀行鍵を個別化、可変化することができ、これにより万一の場合の各種カード

16

偽造行為に対して、カードシステムの安全性向上に寄与するところが大きい。

【0074】

【発明の効果】以上詳述したように、本発明の電子財布システムの鍵管理方式によれば、銀行鍵を個別化、可変化することができ、これにより万一の場合の各種カード偽造行為に対してカードシステムの安全性向上においに寄与するという利点がある。

【図面の簡単な説明】

【図1】本発明の原理説明図である。

【図2】本発明の一実施例における現金自動支払い装置とＩＣカードとの間での鍵生成パラメータ配送処理要領を説明する図である。

【図3】本発明の一実施例におけるＩＣカードと店舗取引端末との間での鍵生成パラメータ配送処理要領を説明する図である。

【図4】本発明の一実施例におけるＩＣカードへの暗号化鍵補給配送処理要領を説明する図である。

【図5】顧客に発行する銀行鍵の変更周期例を説明する図である。

【図6】本発明の電子財布システムの概略を示すブロック図である。

【図7】従来方式によるＩＣカードを用いたプリペイドカード・システムの構成図である。

【図8】従来の店舗側の取引端末の売上合算データの更新とＩＣカード残高の更新の説明図である。

【図9】店舗側の取引端末での売上合算データの更新を説明するシステム構成図である。

【図10】買物客のＩＣカードによる売上合算データの更新を説明するシステム構成図である。

【図11】前回請求データの複写による売上の水増しの説明図である。

【図12】店舗売上データへのシリアル番号の付加説明図である。

【図13】他の店舗取引端末の請求データの複写による売上の水増しの説明図である。

【図14】店舗売上データへの取引端末ＩＤの付加説明図である。

【符号の説明】

2　ＩＣカード
2－1，2－1′，2－1′′，2－1′′′　復号部
2－2，2－2′　加算部
2－3　第1のレジスタ
2－4　第2のレジスタ
2－5　メモリ
2－6　レジスタ
3　店舗取引端末
3－11，3－11′　セキュリティブラックボックス
4　銀行センタ
4Ａ　現金自動支払い装置（ＡＴＭ）

17

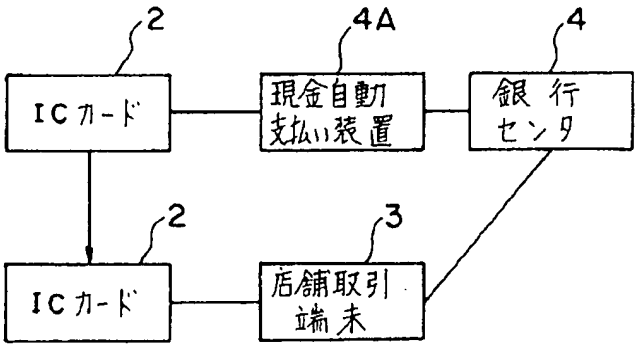
８　残高格納レジスタ
２０　減算器
２０　金額表示部
２１　金額表示部
２２　売上データ
２３　加算器
２４，２５　暗号化部
２６　比較器
２７　銀行鍵
３０　合算データ暗号化部
３１　カード残高更新部
３２　加算器
３３　暗号化部
３４　復号部
３５　比較器
３６　銀行鍵格納部
３７　売上データ格納部

18

３８　加算器
３９　比較器
４５　暗合化部
４６　銀行鍵
４７　比較器
８１　ＩＣカード
８２　店舗取引端末
８３　銀行センタ
８４　個人口座
８５　個人カード残高ログファイル
８６　未決済資金ファイル
８７　店舗口座
８８　残高格納レジスタ
９６　加算器
９７　減算器
９８　金額表示ディスプレイ

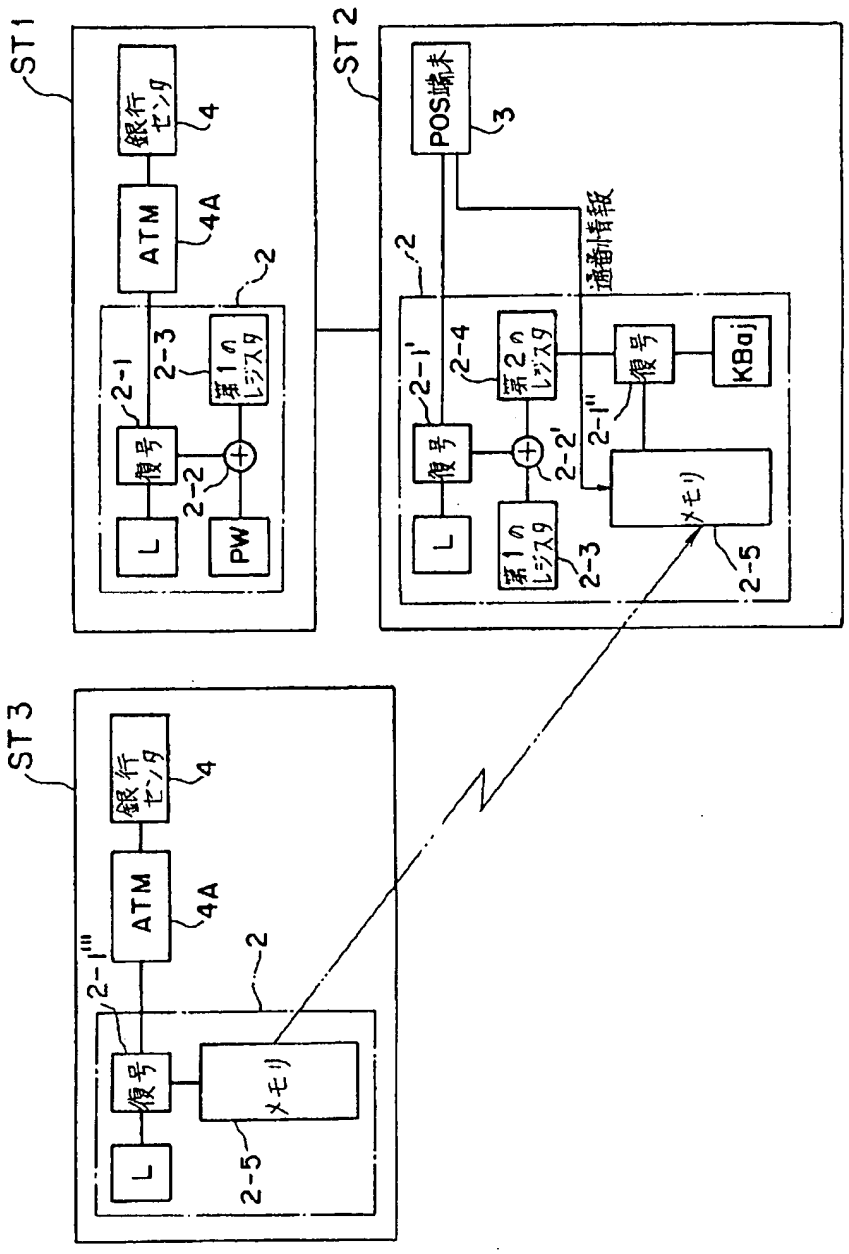
【図６】

本発明の電子財布システムの概略を示すブロック図



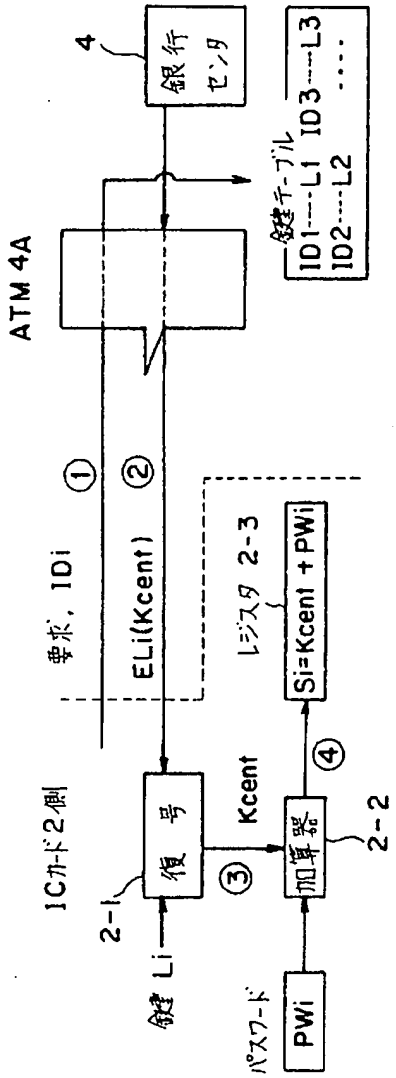
【図1】

本発明の原理説明図



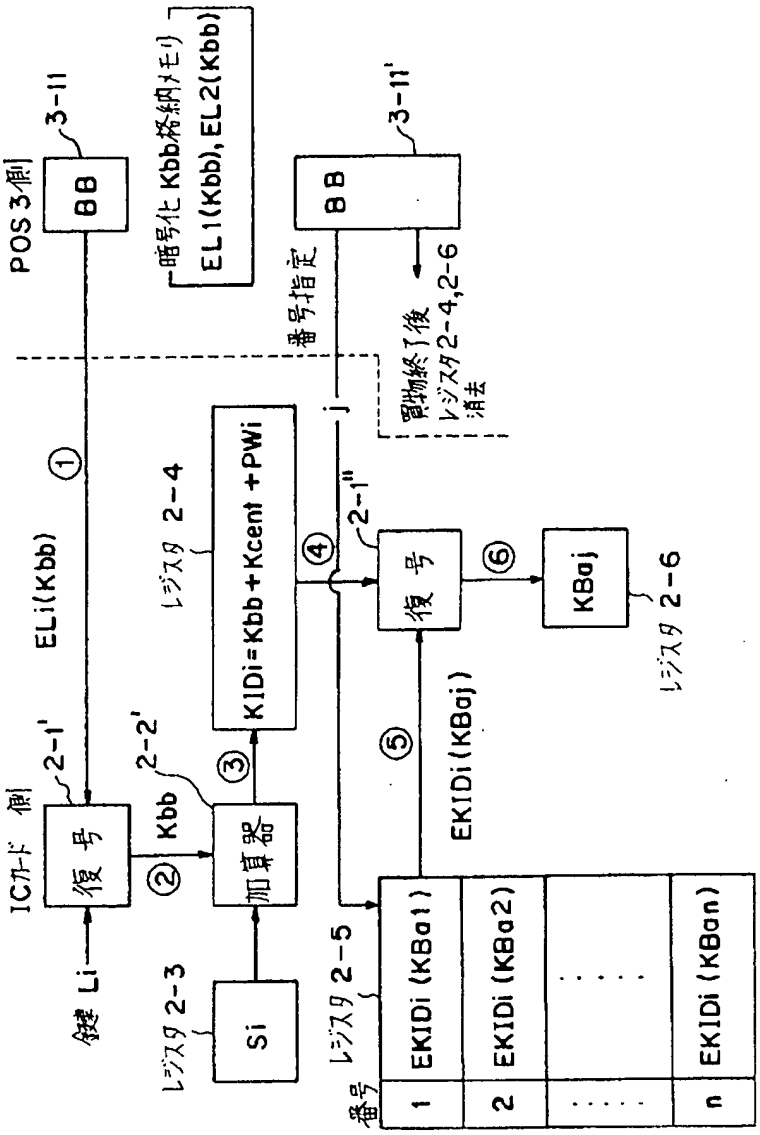
【図2】

本発明の一実施例における現金自動支払い装置とICカードとの間での鍵生成パラメータ配送処理要領を説明する図



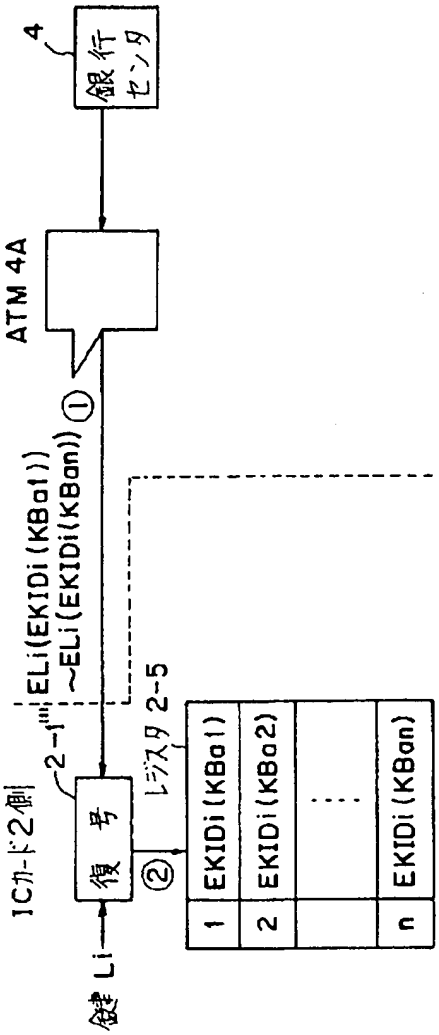
【図3】

本発明の一実施例におけるICカードと店舗取引端末との間での鍵生成パラメータ配送処理要領を説明する図



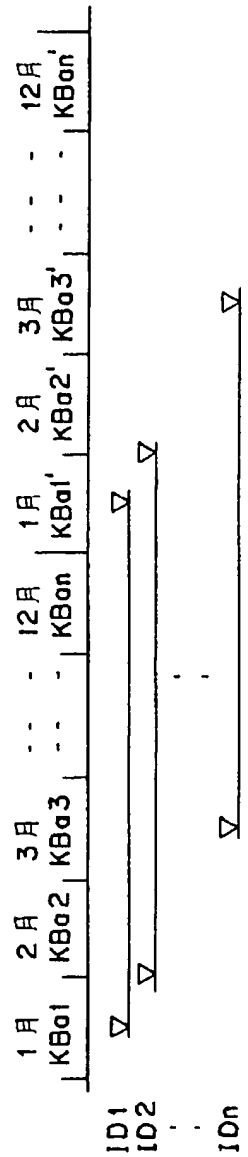
【図4】

本発明の一実施例におけるICカードへの暗号化鍵補給配送処理要領を説明する図



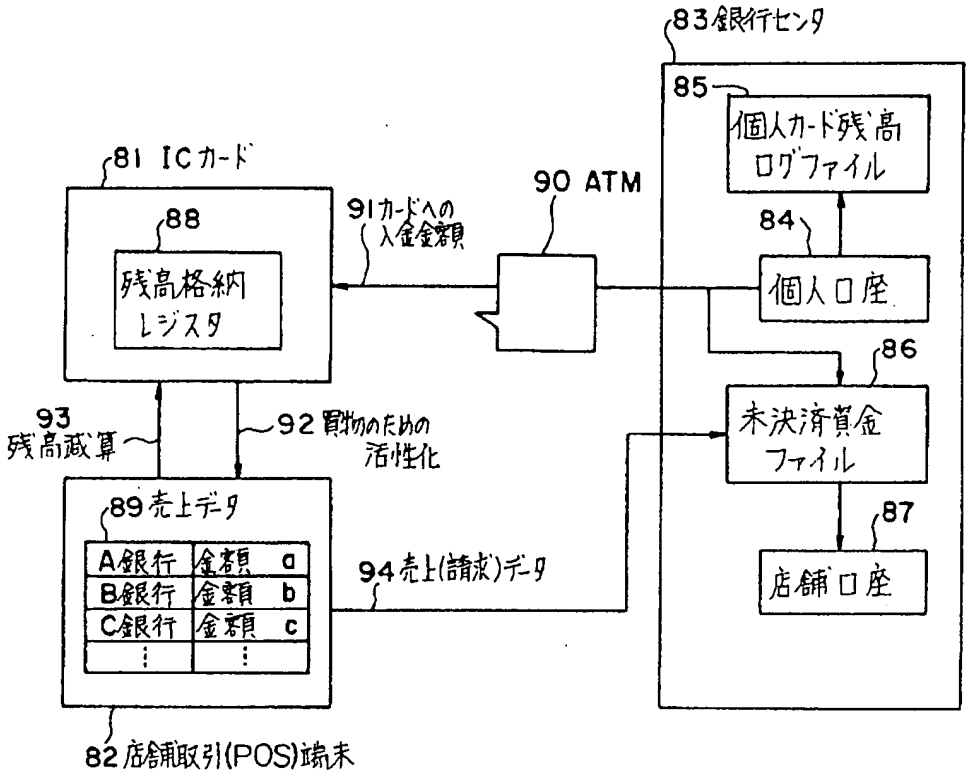
【図5】

顧客に発行する銀行鍵の変更周期例を説明する図



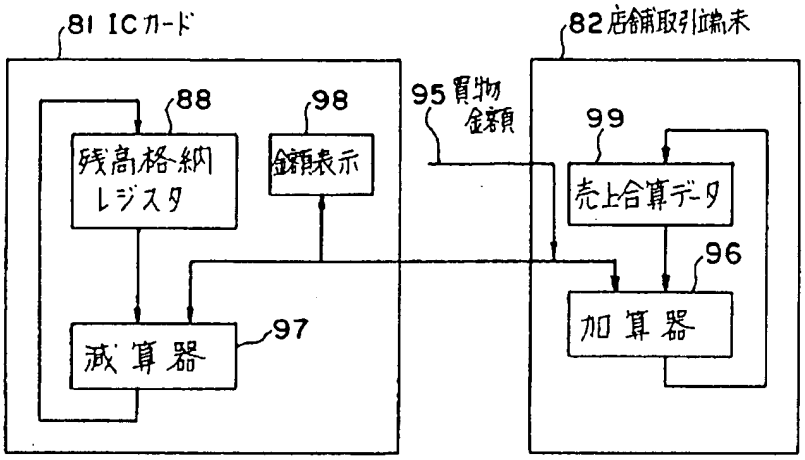
【図7】

従来方式によるICカードを用いたプリペイドカード・システムの構成図



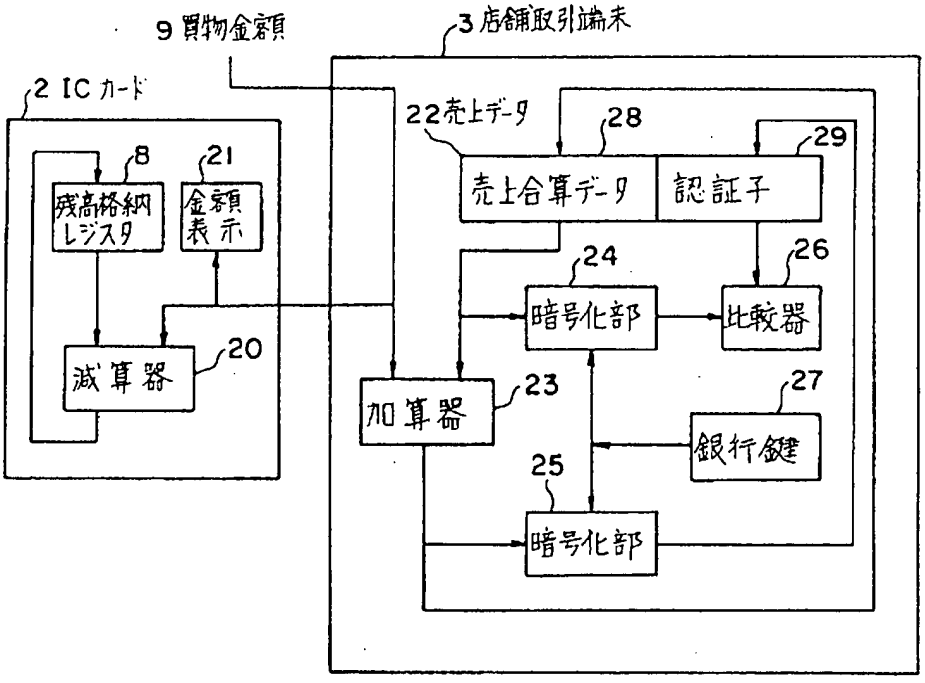
【図8】

従来の店舗側の取引端末の売上合算データの更新と
ICカード残高の更新の説明図



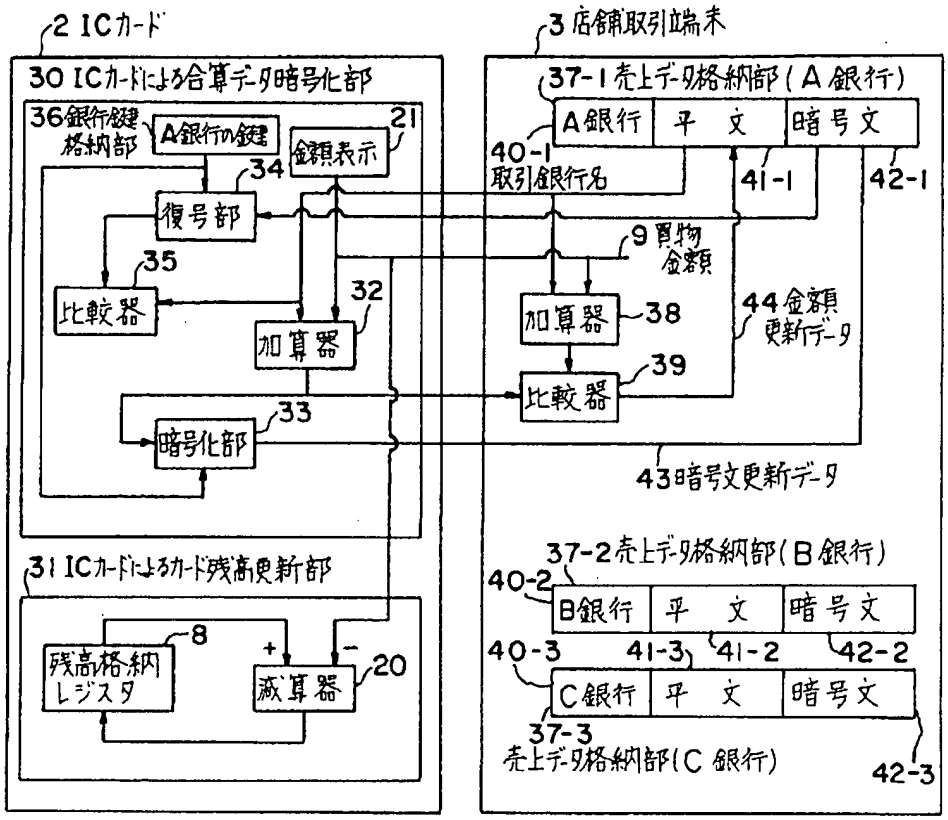
【図9】

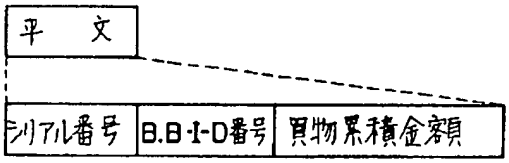
店舗側の取引端末での売上合算データ更新例を説明する
システム構成図



【図10】

買物客のICカードによる売上合算データの更新を説明するシステム構成図



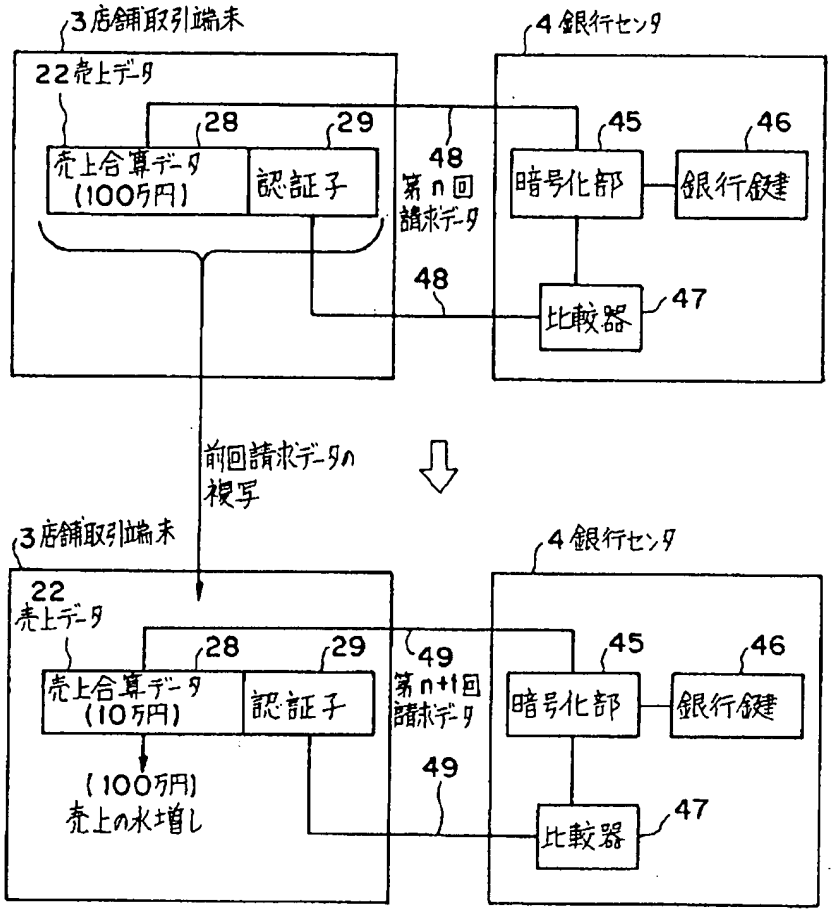


シリアル番号：前回締め上げの以前のデータの利用防止の為のシリアル番号．締め上げの度にインクリメントされる．

B.B-I-D番号：他のブラックボックスの買物累積金額の利用防止の為のID．

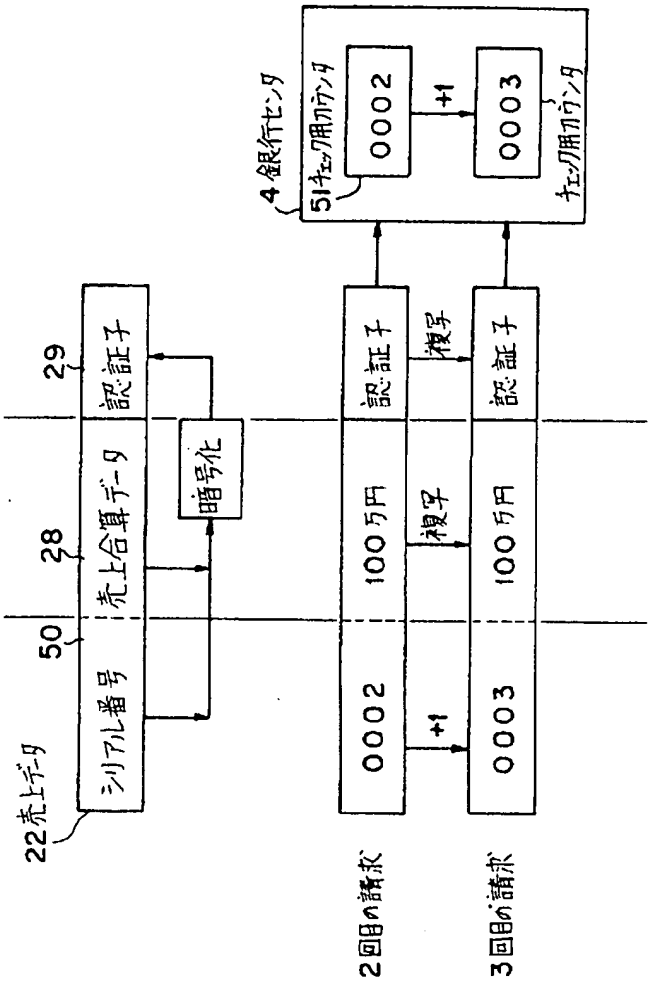
【図11】

前回請求データの複写による売上の水増しの説明図



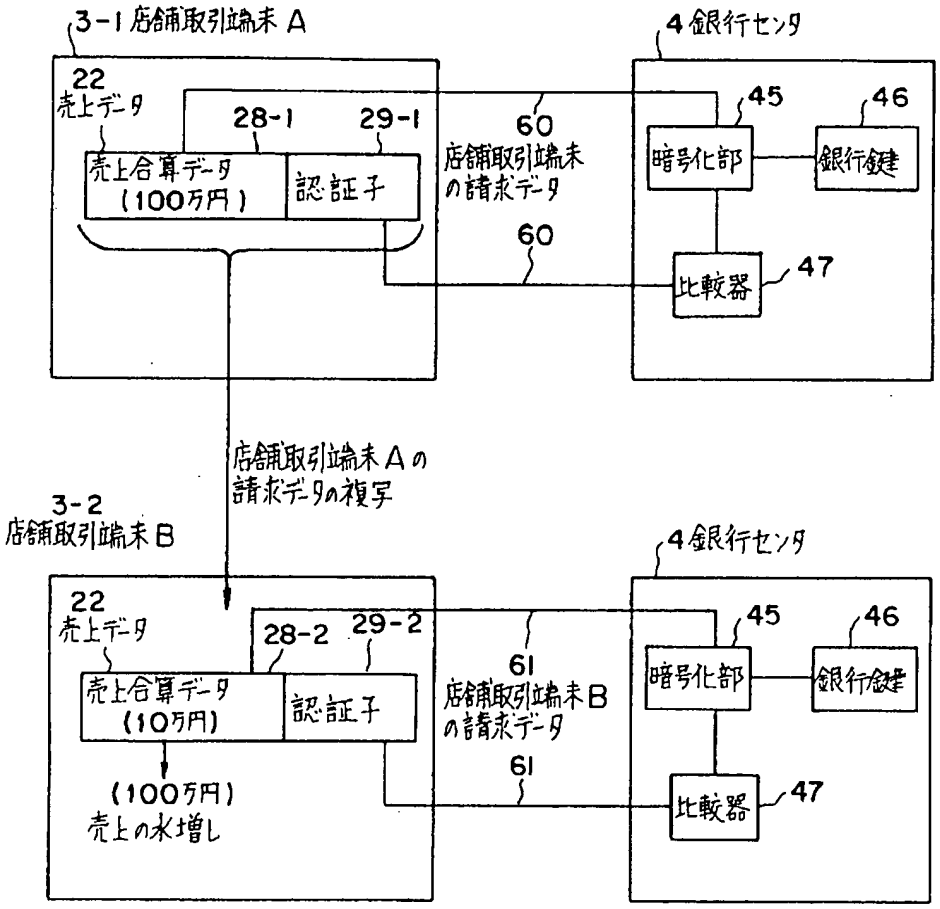
【図12】

店舗売上データへのシリアル番号の付加説明図



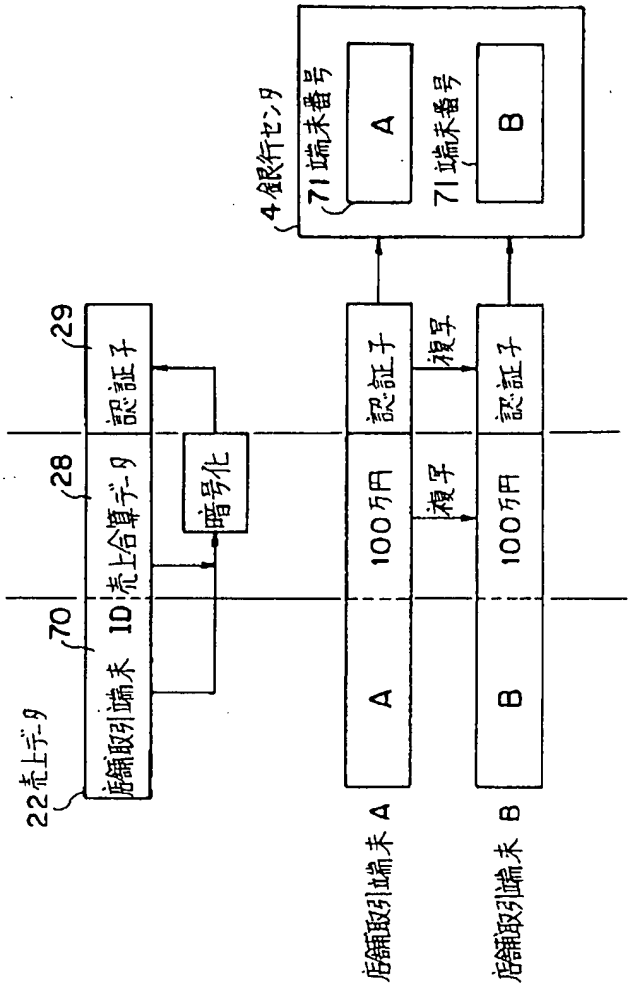
【図13】

他の店舗取引端末の請求データの複写による売上の水増しの説明図



【図14】

店舗売上データへの取引端末IDの付加説明図



フロントページの続き

(51) Int. Cl.[5]		識別記号	庁内整理番号	FI	技術表示箇所
G07D	9/00	461 B	8513－3E		
G07F	7/12				
G07G	1/14		8921－3E		
H04L	9/28				